UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/489,192	01/20/2000	SCOTT A. FIELD	MSI-407US	5535

22801 7590 01/05/2005

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/489,192	FIELD, SCOTT A.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 November 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-26,28-30,32-42 and 44-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-26,28-30,32-42 and 44-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on November 15, 2004. Claims 1, 4 – 26, 28 – 30, 32 – 42 and 44 – 48 were received for consideration. Claims 1, 4 – 26, 28 – 30, 32 – 42 and 44 – 48 were previously presented and no new were added. Claims 1, 4 – 26, 28 – 30, 32 – 42 and 44 – 48 are currently being considered.

Response to Arguments

2. Applicant's arguments filed November 15, 2004 have been fully considered. Applicant's arguments with respect to Claims 1, 4 – 26, 28 – 30, 32 – 42 and 44 – 48 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 4 – 26, 28 – 30, 32 – 42 and 44 – 48 are rejected under 35 U.S.C. 102(e) as being anticipated by Herbert et al. (U.S. Patent Number 6,708,274).

Regarding Claim 1, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), a computer-implemented method of protecting information comprising:

creating a key and page locking the key in the physical memory wherein creating the key comprises creating the key during system boot up, wherein different keys can be created during different system boot ups (Column 2 line 40 – Column 3 line 43 and Column 4 lines 13 – 25);

encrypting information using the key; and paging out, to the page file, the encrypted information (Column 2 line 55 – Column 3 line 3; Column 4 lines 60 – 65 and Column 6 lines 59 – 65).

Regarding Claim 11, Herbert teaches and describes in a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), a computer-implemented method of protecting information comprising:

creating a key during system boot up, wherein different keys can be created during different system boot ups (Column 2 line 40 – Column 3 line 43 and Column 4 lines 13 – 25);

page-locking the key in main memory (Column 3 lines 33 – 43 and Column 4 lines 13 – 28);

restricting access to the page-locked key to only the operating system kernel (Column 2 lines 40 – 48 and Column 3 lines 33 – 43);

calling the operating system kernel to encrypt information (Column 2 line 40 – Column 3 line 43 and Column 4 lines 7 – 25);

accessing the page-locked key with the operating system kernel (Column 4 line 7 – Column 5 line 57); and

using the operating system kernel to encrypt the information with the page-locked key (Column 4 line 7 – Column 5 line 57).

Regarding Claim 19, Herbert teaches and describes in a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), a computer-implemented method of handling encrypted information comprising:

accessing encrypted information in the page file (Column 2 line 55 – Column 3 line 9); and

decrypting the encrypted information with a key created during system boot up, wherein different keys can be created during different system boot ups and wherein the key is page-locked in the main memory (Column 2 line 55 – Column 3 line 9; Column 4 lines 7 – 25 and Column 7 lines 39 – 49).

Regarding Claim 25, Herbert teaches and describes in a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), a computer-implemented method of handling encrypted information comprising:

allocating a non-pageable page of main memory during system boot (Column 1 lines 25 – 40 and Column 2 line 40 – Column 3 line 28);

generating a random key, wherein different keys can be generated during different system boots (Column 2 line 40 – Column 3 line 43 and Column 4 lines 13 – 25); and

storing the random key in the non-pageable page of main memory, the random key being configured for use by the operating system to encrypt information that might be paged out to the page file (Column 2 line 40 – Column 3 line 43; Column 5 lines 26 – 65 and Column 7 lines 39 – 53).

Regarding Claim 30, Herbert teaches and describes in an operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), a computer-implemented method of protecting information comprising:

generating at least one non-pageable random key by using a random key generating process during system boot up, wherein different keys can be generated

during different system boot ups (Column 2 line 40 – Column 3 line 43 and Column 4 lines 13 – 25);

encrypting at least one selected block of information in the main memory with a software component that uses the at least one random key for encryption (Column 2 line 55 – Column 3 line 3; Column 4 lines 60 – 65 and Column 6 lines 59 – 65);

transferring the one encrypted block of information to the secondary storage (Column 2 line 55 – Column 3 line 43; Column 4 lines 60 – 65 and Column 6 lines 59 – 65).

decrypting the one encrypted block of information with the software component that uses the at least one random key for decryption (Column 2 line 55 – Column 3 line 9; Column 4 lines 7 – 25 and Column 7 lines 39 – 49).; and

placing the decrypted block of information in the main memory (Column 3 lines 33 – 43 and Column 5 lines 53 – 67).

Regarding Claim 36, Herbert teaches and describes a system for use in protecting pageable information (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), comprising:

a memory having pageable and non-pageable pages (Column 1 lines 25 – 40 and Column 2 line 40 – Column 3 line 28); and

at least one key created during system boot and stored in the memory in a non-pageable page, the key being configured for use in encrypting pageable information,

wherein different keys can be created during different system boots (Column 2 line 40 – Column 3 line 43 and Column 4 lines 13 – 25);

Regarding Claim 41, Herbert teaches and describes in a computer program embodied on one or more computer-readable media, the program comprising:

creating a key and page locking the key in main memory of a computer, wherein creating the key comprises creating the key during system boot up, wherein different keys can be created during different system boot ups (Column 2 line 40 – Column 3 line 43 and Column 4 lines 13 – 25);

encrypting information with the key (Column 2 line 55 – Column 3 line 3; Column 4 lines 60 – 65 and Column 6 lines 59 – 65);

paging out, to secondary storage, the encrypted information (Column 2 line 55 – Column 3 line 3; Column 4 lines 60 – 65 and Column 6 lines 59 – 65);

accessing the encrypted information in the secondary storage (Column 2 line 55 – Column 3 line 9); and

decrypting the encrypted information with the key that is page-locked in the main memory (Column 2 line 55 – Column 3 line 9; Column 4 lines 7 – 25 and Column 7 lines 39 – 49).

Regarding Claim 42, Herbert teaches and describes a programmable computer comprising:

a processor (Column 2 lines 40 – 44);

main memory for holding information (Column 1 lines 25 – 40 and Column 2 line 40 – Column 3 line 28);

secondary storage for receiving information that is temporarily transferred out of the main memory (Column 2 lines 40 – Column 3 line 43);

the computer being programmed with computer-readable instructions which, when executed by the processor, cause the computer to:

generate a key during system boot up, wherein different keys can be generated during different system boot ups (Column 2 line 40 – Column 3 line 43 and Column 4 lines 13 – 25);

page lock the key in the main memory (Column 3 lines 33 – 43 and Column 4 lines 13 – 28);

encrypt information that is to be transferred to the secondary storage with the key (Column 2 line 55 – Column 3 line 3; Column 4 lines 60 – 65 and Column 6 lines 59 – 65);

transfer the encrypted information to the secondary storage (Column 2 line 55 – Column 3 line 9); and

decrypt the encrypted information with a key that is locked in the main memory (Column 2 line 55 – Column 3 line 9; Column 4 lines 7 – 25 and Column 7 lines 39 – 49).

Regarding Claim 47, Herbert teaches and describes one or more application programming interfaces embodied on one or more computer-readable media for

execution on a computer in conjunction with a paging operating system having main memory for holding information and a page file for receiving information that is paged out from the main memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), comprising:

an interface method for generating a key during system boot up, wherein different keys can be generated during different system boot ups (Column 2 line 40 – Column 3 line 43 and Column 4 lines 13 – 25);

an interface method for page locking the key in the main memory (Column 1 lines 25 – 40 and Column 2 line 40 – Column 3 line 28);

an interface method for encrypting pageable information with the key (Column 2 line 55 – Column 3 line 3; Column 4 lines 60 – 65 and Column 6 lines 59 – 65)and

an interface method for decrypting encrypted information that is contained in the page file (Column 2 line 55 – Column 3 line 9; Column 4 lines 7 – 25 and Column 7 lines 39 – 49).

Regarding Claim 48, Herbert teaches and describes an application programming interface embodied on a computer-readable medium for execution on a computer in conjunction with a paging operating system having main memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the main memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), comprising a method for setting an attribute on a page of main memory, the attribute designating that the page must be encrypted with a key created during system

boot up and locked in the main memory prior to the page being paged out to the page file, wherein different keys can be created during different system boot ups (Column 1 lines 25 – 40; Column 2 line 40 – Column 3 line 43 and Column 4 lines 13 – 25).

Claim 4 is rejected as applied above in rejecting Claim 1. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), wherein said creating the key further comprises generating a random key with a random key generator (Column 2 line 40 – Column 3 line 43 and Column 4 lines 13 – 25).

Claims 6 and 22 are rejected as applied above in rejecting Claims 1 and 19. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), wherein said encrypting comprises:

calling an operating system kernel (Column 2 line 40 – Column 3 line 43);

the kernel using the page-locked key to encrypt the information (Column 2 line 40 – Column 3 line 43 and Column 5 lines 53 – 67).

Claims 9, 17, 23 and 28 are rejected as applied above in rejecting Claims 1, 11, 19 and 25. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), one or more computer-readable media having computer-readable instructions thereon which, when executed by a computer, perform the computer-implemented method of Claims 1, 11, 19, 25 and 11 (Column 2 line 40 – Column 3 line 43 and Column 5 lines 53 – 67).

Claims 10, 18, 24, 29 and 35 are rejected as applied above in rejecting Claims 1, 11, 19, 25 and 30. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), an operating system programmed with instructions which, when implemented by the operating system, implemented the method of claims 1 and 11 (Column 2 line 40 – Column 3 line 43 and Column 5 lines 53 – 67).

Claim 14 is rejected as applied above in rejecting Claim 11. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving

information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), further comprising prior to said calling:

designating at least one page in the main memory with a designation (Column 1 lines 25 – 40 and Column 2 line 40 – Column 3 line 28);

recognizing the designation and, responsive thereto, calling the operating system kernel to encrypt the information (Column 2 line 40 – Column 3 line 43 and Column 5 lines 53 – 67).

Claim 16 is rejected as applied above in rejecting Claim 11. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), wherein said calling comprises specifying a memory location and a memory size associated with the information to be encrypted (Column 3 line 33 – Column 4 line 6).

Claim 20 is rejected as applied above in rejecting Claim 19. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), further comprising placing the decrypted information in a page of main memory (Column 3 lines 3 – 9).

Claim 21 is rejected as applied above in rejecting Claim 19. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), further comprising placing the decrypted information in a page-locked page of main memory (Column 2 line 55 – Column 3 line 9).

Claims 32, 37, 38, 39 and 40 are rejected as applied above in rejecting Claims 30 and 36. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), further comprising restricting access to the at least one random key to only the software component (Column 4 lines 15 – 28 and Column 5 lines 34 – 67).

Claim 33 is rejected as applied above in rejecting Claim 30. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), wherein the software component comprises

the operating system's kernel (Column 2 line 40 – Column 3 line 43; Column 4 lines 7 – 28 and Column 5 lines 34 – 67).

Claim 34 is rejected as applied above in rejecting Claim 30. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), further comprising:

storing the at least one random key in the main memory (Column 3 lines 33 – 43 and Column 4 lines 13 – 28); and

locking the at least one random key in the main memory so that it does not get transferred to the second storage (Column 2 line 40 – Column 3 line 43; Column 5 lines 26 – 65 and Column 7 lines 39 – 53).

Claim 44 is rejected as applied above in rejecting Claim 42. Furthermore, Herbert teaches and describes a programmable computer, wherein the key that is used to encrypt the information is the same key that is used to decrypt the information (Column 3 lines 3 – 25).

Claim 45 is rejected as applied above in rejecting Claim 42. Furthermore, Herbert teaches and describes a programmable computer, further comprising a software

component that is programmed to encrypt and decrypt the information (Column 3 lines 3 – 25 and Column 5 lines 34 – 67)

Claims 5 and 26 are rejected as applied above in rejecting Claims 4 and 25. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), wherein said generating comprises using RSA RC4 as an encryption algorithm to generate the key (Column 3 lines 16 – 32).

Claims 7 and 13 are rejected as applied above in rejecting Claims 6 and 11. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b; Summary and Column 2 line 26 – Column 7 line 53), wherein said calling is performed by an application (Column 2 line 40 – Column 3 line 43 and Column 5 lines 53 – 67).

Claims 8, 12 and 15 are rejected as applied above in rejecting Claims 1, 11 and 14. Furthermore, Herbert teaches and describes in a paging operating system having physical memory for holding information and secondary storage comprising a page file for receiving information that is paged out from the physical memory (Fig. 1 – 3, 5a, 5b;

Summary and Column 2 line 26 – Column 7 line 53), wherein said calling is performed by an operating system memory manager (Column 2 line 40 – Column 3 line 43 and Column 5 lines 53 – 67).

Claim 46 is rejected as applied above in rejecting Claim 45. Furthermore, Herbert teaches and describes a programmable computer, wherein the software component comprises the operating system's kernel (Column 2 line 40 – Column 3 line 43 and Column 5 lines 34 – 67).

Conclusion

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
December 28, 2004.

EMMANUEL L. MOISE
PRIMARY EXAMINER